Departament d'Informàtica

Programació Didàctica
Ciberseguretat en entorns de les tecnologíes de la informació

Curs d'especialització

Programació

IES Jaume II el Just

Tavernes de la Valldigna

Índex

1 Introducció. Justificació i contextualització

Reial Decret del Títol 405/2023

ORDE EDU/2000/2010 Currículum

FPB Informàtica d'Oficina:

- ☐ RD 356/2014, de 16 de mayo
- ☐ Currículo CV: DECRETO 185/2014, de 31 de octubre

SMX:

- ☐ RD 1691/2007, de 14 de diciembre
- ☐ ORDE de 29 de juliol de 2009

ASIX:

- ☐ RD 1629/2009, de 30 de octubre
- ☐ ORDEN 36/2012, de 22 de junio

DAM:

- ☐ RD 450/2010, de 16 de abril
- ☐ Reial Decret del Títol 405/2023
- ☐ ORDEN 58/2012, de 5 de septiembre

DAW:

- ☐ RD 686/2010, de 20 de mayo
- ☐ Reial Decret del Títol 405/2023
- ☐ ORDEN 60/2012, de 25 de septiembre

Curs d'especialització:

- [x] Ciberseguridad
  - [x] RD 479/2020, de 7 d'abril
- ☐ BigData

- ☐ RD 279/2021, de 20 d'abril

El títol d'especialista en **ciberseguretat en entorns de les tecnologíes de la informació** queda identificat pels elements següents:

Denominació: Ciberseguretat en entorns de les tecnologíes de la informació.

Nivell: Formació Professional de Grau Superior.

Durada: 720 hores.

Equivalència en crèdits ECTS: 43.

Família professional: Informàtica i Comunicacions.

Branques de coneixement: Ciències. Enginyeria i arquitectura.

Referent a la ClassificacióInternacional Normalitzada de l'Educació: P-5.5.4.

Nivell del Marc Espanyol de Qualificacions per a l'EducacióSuperior: Nivell 1 Tècnic Superior.

2 Competències

2.1 Competència general

La competència general d'este curs d'especialització consistix a definir i implementar estratègies de seguretat en els sistemes d'informació realitzant diagnòstics de ciberseguretat, identificant vulnerabilitats i implementant les mesures necessàries per a mitigar-les aplicant la normativa vigent i estàndards del sector, seguint els protocols de qualitat, de prevenció de riscos laborals i respecte ambiental.

2.2 Competències professionals, personals i socials

a) Elaborar i implementar plans de prevenció i conscienciació en ciberseguretat en l'organització, aplicant la normativa vigent.
b) Detectar i investigar incidents de ciberseguretat, documentant-los i incloent-los en els plans de protecció de l'organització.
c) Dissenyar plans de protecció contemplant les millors pràctiques per al *bastionado de sistemes i xarxes.

d) Configurar sistemes de control d'accés i autenticació en sistemes informàtics, complint els requisits de seguretat i minimitzant les possibilitats d'exposició a atacs.
e) Dissenyar i administrar sistemes informàtics en xarxa i aplicar les polítiques de seguretat establides, garantint la funcionalitat requerida amb un nivell de risc controlat.
f) Analitzar el nivell de seguretat requerit per les aplicacions i els vectors d'atac més habituals, evitant incidents de ciberseguretat.
g) Implantar sistemes segurs de desplegat de programari amb l'adequada coordinació entre els desenrotlladors i els responsables de l'operació del programari.
h) Realitzar anàlisi forenses informàtics analitzant i registrant la informació rellevant relacionada.
i) Detectar vulnerabilitats en sistemes, xarxes i aplicacions, avaluant els riscos associats.
j) Definir i aplicar procediments per al compliment normatiu en matèria de ciberseguretat i de protecció de dades personals, implementant-los tant internament com en relació amb tercers.
k) Elaborar documentació tècnica i administrativa complint amb la legislació vigent, responent als requisits establits.
l) Adaptar-se a les noves situacions laborals, mantenint actualitzats els coneixements científics, tècnics i tecnològics relatius al seu entorn professional, gestionant la seua formació i els recursos existents en l'aprenentatge al llarg de la vida.
m) Resoldre situacions, problemes o contingències amb iniciativa i autonomia en l'àmbit de la seua competència, amb creativitat, innovació i esperit de millora en el treball personal i en el dels membres de l'equip.
n) Generar entorns segurs en el desenrotllament del seu treball i el del seu equip, supervisant i aplicant els procediments de prevenció de riscos laborals i ambientals, d'acord amb el que s'establix per la normativa i els objectius de l'organització. ñ) Supervisar i aplicar procediments de gestió de qualitat, d'accessibilitat universal i de «disseny per a totes les persones», en les activitats professionals incloses en els processos de producció o prestació de servicis.

2.3 Relació de qualificacions i unitats de competència

Qualificació Professional Completa:

Qualificacions Professionals Incompletes:

3 Objectius generals del cicle

Els objectius generals del cicle formatiu són els següents:

a) Identificar els principis de l'organització i normativa de protecció en ciberseguretat, planificant les accions que cal adoptar en el lloc de treball per a l'elaboració del pla de prevenció i

conscienciació.

b) Auditar el compliment del pla de prevenció i conscienciació de l'organització, definint les accions correctores que puguen derivar-se per a incloure-les en el pla es protecció de l'organització.
c) Detectar incidents de ciberseguretat implantant els controls, les ferramentes i els mecanismes necessaris per al seu monitoratge i identificació.
d) Analitzar i donar resposta a incidents de ciberseguretat, identificant i aplicant les mesures necessàries per a la seua mitigació, eliminació, contenció o recuperació.
e) Elaborar anàlisi de riscos per a identificar actius, amenaces, vulnerabilitats i mesures de seguretat.
f) Dissenyar i implantar plans de mesures tècniques de seguretat a partir dels riscos identificats per a garantir el nivell de seguretat requerit.
g) Configurar sistemes de control d'accés, autenticació de persones i administració de credencials per a preservar la privacitat de les dades.
h) Configurar la seguretat de sistemes informàtics per a minimitzar les probabilitats d'exposició a atacs.
i) Configurar dispositius de xarxa per a complir amb els requisits de seguretat.
j) Administrar la seguretat de sistemes informàtics en xarxa aplicant les polítiques de seguretat requerides per a garantir la funcionalitat necessària amb el nivell de risc de xarxa controlat.
k) Aplicar estàndards de verificació requerits per les aplicacions per a evitar incidents de seguretat.
l) Automatitzar plans de desplegat de programari respectant els requisits relatius a control de versions, rols, permisos i altres per a aconseguir un desplegat segur.
m) Aplicar tècniques d'investigació forense en sistemes i xarxes en els àmbits de l'emmagatzematge de la informació no volàtil, dels dispositius mòbils, del *Cloud i dels sistemes* IoT (Internet de les coses), entre altres, per a l'elaboració d'anàlisi forenses.
n) Analitzar informes forenses identificant els resultats de la investigació per a extraure conclusions i realitzar informes. ñ) Combinar tècniques de *hacking ètic intern i extern per a detectar vulnerabilitats que permeten eliminar i mitigar els riscos associats.
o) Identificar l'abast de l'aplicació normativa dins de l'organització, tant internament com en relació amb tercers per a definir les funcions i responsabilitats de totes les parts.
p) Revisar i actualitzar procediments d'acord amb normes i estàndards actualitzats per al correcte compliment normatiu en matèria de ciberseguretat i de protecció de dades personals.
q) Desenrotllar manuals d'informació, utilitzant ferramentes ofimàtiques i de disseny assistit per ordinador per a elaborar documentació tècnica i administrativa.
r) Analitzar i utilitzar els recursos i oportunitats d'aprenentatge relacionats amb l'evolució científica, tecnològica i organitzativa del sector i les tecnologies de la informació i la comunicació, per a mantindre l'esperit d'actualització i adaptar-se a noves situacions laborals i personals.
s) Desenrotllar la creativitat i l'esperit d'innovació per a respondre als reptes que es presenten en els processos i en l'organització del treball i de la vida personal.

t) Avaluar situacions de prevenció de riscos laborals i de protecció ambiental, proposant i aplicant mesures de prevenció personals i col·lectives, d'acord amb la normativa aplicable en els processos de treball, per a garantir entorns segurs.
u) Identificar i proposar les accions professionals necessàries per a donar resposta a l'accessibilitat universal i al «disseny per a totes les persones».
v) Identificar i aplicar paràmetres de qualitat en els treballs i activitats realitzats en el procés d'aprenentatge, per a valorar la cultura de l'avaluació i de la qualitat i ser capaces de supervisar i millorar procediments de qualitat.

4 Mòduls professionals del cicle

4.1 1r curs

Els mòduls es cursen en 2 quatrimestres.

Codi	Mòdul	hrs/set	hrs/any
5021	Incidents de coberseguretat	4	120
5022	Bastionat de xarxes i sistemes	7	210
5023	Posada en producció segura	4	120
5024	Anàlisi forense informàtic.	4	120
5025	Hacking ètic.	4	120
5026	Normativa de ciberseguretat.	1	30

5 Resultats d'aprenentatge

5.1 Els resultats d'aprenentatge del mòdul

Resultats d'aprenentatge	
RA1	Desenvolupa plans de prevenció i conscienciació en ciberseguretat, establint normes i mesures de protecció.
RA2	Analitza incidents de ciberseguretat utilitzant ferramentes, mecanismes de detecció i alertes de seguretat.
RA3	Investiga incidents de ciberseguretat analitzant els riscos implicats i definint les possibles mesures a adoptar
RA4	Implementa mesures de ciberseguretat en xarxes i sistemes responent als incidents detectats i aplicant les tècniques de protecció adequades.
RA5	Detecta i documenta incidents de ciberseguretat seguint procediments d'actuació establerts.

Figura 1: RA - IC

5.2 Relació entre els resultats d'aprenentatge i els criteris d'avaluació

Sistemes de Gestió Empresarial								
Unitats didàctiques		RA1	RA2	RA3	RA4	RA5		
1	Desenvolupament de plans de prevenció i conscienciació en ciberseguretat	a,b,c,d,e						C1
2	Auditoria d'incidents de ciberseguretat		a,b,c,d,e					C2
3	Investigació dels incidents de ciberseguretat			a,b,c,d,e				C4
4	Implementació de mesures de ciberseguretat				a,b,c,d,e,f			C3
5	Detecció i documentació d'incidents de ciberseguretat					a,b,c,d,e		C5

Resultats d'aprenentatge i criteris d'avaluació		
RA1	Desenvolupa plans de prevenció i conscienciació en ciberseguretat, establint normes i mesures de protecció.	**RA1**.a)S'han definit els principis generals de l'organització en matèria de ciberseguretat, que han de ser coneguts i secundats per la direcció d'esta. **RA1**.b) S'ha establit una normativa de protecció del lloc de treball. **RA1**.c)S'ha definit un pla de conscienciació de ciberseguretat dirigit als empleats. **RA1**.d) S'ha desenrotllat el material necessari per a dur a terme les accions de conscienciació dirigides als empleats. **RA1**.e) S'ha realitzat una auditoria per a verificar el compliment del pla de prevenció i conscienciació de l'organització.
RA2	Analitza incidents de ciberseguretat utilitzant ferramentes, mecanismes de detecció i alertes de seguretat.	**RA2**.a)S'ha classificat i definit la taxonomia d'incidents de ciberseguretat que poden afectar l'organització. **RA2**.b) S'han establit controls, ferramentes i mecanismes de monitoratge, identificació, detecció i alerta d'incidents **RA2**.c)S'han establit controls i mecanismes de detecció i identificació d'incidents de seguretat física. **RA2**.d) S'han establit controls, ferramentes i mecanismes de monitoratge, identificació, detecció i alerta d'incidents a través de la investigació en fonts obertes (OSINT: Open Source Intelligence). **RA2**.e)S'ha realitzat una classificació, valoració, documentació i seguiment dels incidents detectats dins de l'organització.
RA3	Investiga incidents de ciberseguretat analitzant els riscos implicats i definint les possibles mesures a adoptar	**RA3**.a) S'han recopilat i emmagatzemat de manera segura evidències d'incidents de ciberseguretat que afecten l'organització. **RA3**.b) S'ha realitzat una anàlisi d'evidències. **RA3**.c) S'ha realitzat la investigació d'incidents de ciberseguretat. **RA3**.d) S'ha intercanviat informació d'incidents, amb proveïdors i/o organismes competents que podrien fer aportacions sobre aquest tema. **RA3**.e) S'han iniciat les primeres mesures de contenció dels incidents per a limitar els possibles danys causats.

RA4	Implementa mesures de ciberseguretat en xarxes i sistemes responent als incidents detectats i aplicant les tècniques de protecció adequades.	**RA4.**a) S'han desenvolupat procediments d'actuació detallats per a donar resposta, mitigar, eliminar o contindre els tipus d'incidents de ciberseguretat més habituals. **RA4.**b) S'han preparat respostes ciberresilientes davant incidents que permeten continuar prestant els servicis de l'organització i enfortint les capacitats d'identificació, detecció, prevenció, contenció, recuperació i cooperació amb tercers. **RA4.**c) S'ha establit un flux de presa de decisions i escalat d'incidents intern i/o extern adequats. **RA4.**d) S'han dut a terme les tasques de restabliment dels servicis afectats per un incident fins a confirmar la volta a la normalitat. **RA4.**e) S'han documentat les accions realitzades i les conclusions que permeten mantindre un registre de "lliçons apreses". **RA4.**f) S'ha realitzat un seguiment adequat de l'incident per a evitar que una situació similar es torne a repetir.
RA5	Detecta i documenta incidents de ciberseguretat seguint procediments d'actuació establerts.	**RA5.**a)S'ha desenvolupat un procediment d'actuació detallat per a la notificació d'incidents de ciberseguretat en els temps adequats. **RA5.**b)S'ha notificat l'incident de manera adequada al personal intern de l'organització responsable de la presa de decisions. **RA5.**c)S'ha notificat l'incident de manera adequada a les autoritats competents en l'àmbit de la gestió d'incidents de ciberseguretat en cas de ser necessari. **RA5.**d)S'ha notificat formalment l'incident als afectats, personal intern, clients, proveïdors, etc., en cas de ser necessari. **RA5.**e)S'ha notificat l'incident als mitjans de comunicació en cas de ser necessari.

6 Contingut. Unitats didàctiques

6.1 Contingut de les unitats didàctiques

Incidents de Ciberseguretat												
Unitats didàctiques		**C1**	**C2**	**C3**	**C4**	**C5**						
1	Desenvolupament de plans de prevenció i conscienciació en ciberseguretat	x										
2	Auditoria d'incidents de ciberseguretat		x									
3	Investigació dels incidents de ciberseguretat			x								
4	Implementació de mesures de ciberseguretat				x							
5	Detecció i documentació d'incidents de ciberseguretat					x						

Continguts	
C1	Desenvolupament de plans de prevenció i conscienciació en ciberseguretat: C1.1 Principis generals en matèria de ciberseguretat. C1.2 Normativa de protecció del lloc del treball. C1.3 Pla de formació i conscienciació en matèria de ciberseguretat. C1.4 Materials de formació i conscienciació. C1.5 Auditories internes de compliment en matèria de prevenció
C2	Auditoria d'incidents de ciberseguretat: C2.1 Taxonomia d'incidents de ciberseguretat C2.2 Controls, ferramentes i mecanismes de monitoratge, identificació, detecció i alerta d'incidents: tipus i fonts C2.3 Controls, ferramentes i mecanismes de detecció i identificació d'incidents de seguretat física. C2.4 Controls, ferramentes i mecanismes de monitoratge, identificació, detecció i alerta d'incidents a través de la investigació en fonts obertes (*OSINT). C2.5 Classificació, valoració, documentació, seguiment inicial d'incidents de ciberseguretat
C3	Investigació dels incidents de ciberseguretat: C3.1 Recopilació d'evidències. C3.2 Anàlisi d'evidències. C3.3 Investigació de l'incident C3.4 Intercanvi d'informació de l'incident amb proveïdors o organismes competents. C3.5 Mesures de contenció d'incidents
C4	Implementació de mesures de ciberseguretat: C4.1 Desenrotllar procediments d'actuació detallats per a donar resposta, mitigar,eliminar o contindre els tipus d'incidents. C4.2 Implantar capacitats de ciberresiliencia. C4.3 Establir fluxos de presa de decisions i escalat intern i/o extern adequats. C4.4 Tasques per a restablir els servicis afectats per incidents. C4.5 Documentació C4.6 Seguiment d'incidents per a evitar una situació similar
C5	Detecció i documentació d'incidents de ciberseguretat: C5.1 Desenrotllar procediments d'actuació per a la notificació d'incidents. C5.2 Notificació interna d'incidents. C5.3 Notificació d'incidents als qui corresponga

6.2 Distribució temporal de les unitats didàctiques

Hores per trimestre, total de trimestres i h anuals establertes.

1r Trimestre	2n Trimestre
60 hores	60 hores
Unitats Didàctiques: UD1, UD2, UD3	Unitats Didàctiques : UD3, UD4, UD5

6.3 Metodologia. Orientacions Didàctiques. Activitats i Estratègies d'ensenyament i aprenentatge.

La metodologia haurà de ser eminentment pràctica, acompanyada de situacions que reflectisquen la realitat en la major mesura possible, ajustant-se al material disponible. Per al treball a l'aula, els alumnes disposaran de tota la documentació que necessiten, a més de l'assistència permanent del professor.

La metodologia serà participativa, afavorint l'aprenentatge per descobriment. Partint dels coneixements inicials dels alumnes/as, estos hauran de construir els seus aprenentatges significatius.

Les **línies d'actuació** en el procés d'ensenyament-aprenentatge que permeten assolir els objectius del mòdul seran:

- Presentació dels continguts. Es relacionen amb els objectius a aconseguir i amb la metodologia a seguir. Es realitzarà una avaluació inicial al principi de cada unitat de treball per a comprovar els coneixements bàsics que poden tindre alguns dels alumnes. Es farà per mitjà de preguntes espontànies a l'aula. Servirà per a construir l'aprenentatge sobre el que saben els alumnes, també per a detectar mites o conceptes erronis que puguen tindre alguns alumnes per endavant.
- Descripció teòrica dels continguts conceptuals. S'utilitzaran, en la mesura que siga possible, els mitjans audiovisuals per a facilitar la seua assimilació. Consistirà en l'exposició en classe de les unitats de treball.
- Exemplificació pràctica dels continguts exposats. Es procurarà relacionar els continguts exposats amb situacions concretes i pròximes a l'entorn sociolaboral de l'alumnat o, amb caràcter més general, a l'actualitat regional, nacional o internacional.
- Es resoldran en classe exercicis i supòsits. Els alumnes podran utilitzar els seus equips per a verificar la correcció de tals suposats. Realització d'activitats de consolidació, individualment i/o en grups de treball. Es podran realitzar en classe i/o a casa (sense donar per descomptat que els alumnes disposen d'ordinador a casa), posteriorment es corregiran per part del professor, ja siga mitjançant posada en comú en classe o individualment fora de l'horari lectiu.
-

7 AVALUACIÓ

Els criteris d'avaluació del mòdul professional Incidents de Ciberseguretat estan associats a resultats d'aprenentatge, definits en el Reial decret que establix el títol. Permeten comprovar el nivell d'adquisició del resultat d'aprenentatge corresponent i constituïxen la guia i el suport per a definir les activitats pròpies del procés d'avaluació.

Apareixen ací de manera general associats a cada resultat d'aprenentatge i concretats en cadascuna de les unitats didàctiques o de treball.

7.1 Criteris d'avaluació

Sistemes de Gestió Empresarial												
Unitats didàctiques		RA1	RA2	RA3	RA4	RA5						
1	Desenvolupament de plans de prevenció i conscienciació en ciberseguretat	a,b,c,d,e						C1				
2	Auditoria d'incidents de ciberseguretat		a,b,c,d,e					C2				
3	Investigació dels incidents de ciberseguretat			a,b,c,d,e				C4				
4	Implementació de mesures de ciberseguretat				a,b,c,d,e,f			C3				
5	Detecció i documentació d'incidents de ciberseguretat					a,b,c,d,e		C5				

Resultats d'aprenentatge i criteris d'avaluació		
RA1	Desenvolupa plans de prevenció i conscienciació en ciberseguretat, establint normes i mesures de protecció.	**RA1.**a)S'han definit els principis generals de l'organització en matèria de ciberseguretat, que han de ser coneguts i secundats per la direcció d'esta. **RA1.**b) S'ha establit una normativa de protecció del lloc de treball. **RA1.**c)S'ha definit un pla de conscienciació de ciberseguretat dirigit als empleats. **RA1.**d) S'ha desenrotllat el material necessari per a dur a terme les accions de conscienciació dirigides als empleats. **RA1.**e) S'ha realitzat una auditoria per a verificar el compliment del pla de prevenció i conscienciació de l'organització.
RA2	Analitza incidents de ciberseguretat utilitzant ferramentes, mecanismes de detecció i alertes de seguretat.	**RA2.**a)S'ha classificat i definit la taxonomia d'incidents de ciberseguretat que poden afectar l'organització. **RA2.**b) S'han establit controls, ferramentes i mecanismes de monitoratge, identificació, detecció i alerta d'incidents **RA2.**c)S'han establit controls i mecanismes de detecció i identificació d'incidents de seguretat física. **RA2.**d) S'han establit controls, ferramentes i mecanismes de monitoratge, identificació, detecció i alerta d'incidents a través de la investigació en fonts obertes (OSINT: Open Source Intelligence). **RA2.**e)S'ha realitzat una classificació, valoració, documentació i seguiment dels incidents detectats dins de l'organització.
RA3	Investiga incidents de ciberseguretat analitzant els riscos implicats i definint les possibles mesures a adoptar	**RA3.**a) S'han recopilat i emmagatzemat de manera segura evidències d'incidents de ciberseguretat que afecten l'organització. **RA3.**b) S'ha realitzat una anàlisi d'evidències. **RA3.**c) S'ha realitzat la investigació d'incidents de ciberseguretat. **RA3.**d) S'ha intercanviat informació d'incidents, amb proveïdors i/o organismes competents que podrien fer aportacions sobre aquest tema. **RA3.**e) S'han iniciat les primeres mesures de contenció dels incidents per a limitar els possibles danys causats.
RA4	Implementa mesures de ciberseguretat en xarxes i sistemes responent als incidents detectats i aplicant les tècniques de protecció adequades.	**RA4.**a) S'han desenvolupat procediments d'actuació detallats per a donar resposta, mitigar, eliminar o contindre els tipus d'incidents de ciberseguretat més habituals. **RA4.**b) S'han preparat respostes ciberresilientes davant incidents que permeten continuar prestant els servicis de l'organització i enfortint les capacitats d'identificació, detecció, prevenció, contenció, recuperació i cooperació amb tercers. **RA4.**c) S'ha establit un flux de presa de decisions i escalat d'incidents intern i/o extern adequats. **RA4.**d) S'han dut a terme les tasques de restabliment dels servicis afectats per un incident fins a confirmar la volta a la normalitat. **RA4.**e) S'han documentat les accions realitzades i les conclusions que permeten mantindre un registre de "lliçons apreses". **RA4.**f) S'ha realitzat un seguiment adequat de l'incident per a evitar que una situació similar es torne a repetir.
RA5	Detecta i documenta incidents de ciberseguretat seguint procediments d'actuació establerts.	**RA5.**a)S'ha desenvolupat un procediment d'actuació detallat per a la notificació d'incidents de ciberseguretat en els temps adequats. **RA5.**b)S'ha notificat l'incident de manera adequada al personal intern de l'organització responsable de la presa de decisions. **RA5.**c)S'ha notificat l'incident de manera adequada a les autoritats competents en l'àmbit de la gestió d'incidents de ciberseguretat en cas de ser necessari. **RA5.**d)S'ha notificat formalment l'incident als afectats, personal intern, clients, proveïdors, etc., en cas de ser necessari. **RA5.**e)S'ha notificat l'incident als mitjans de comunicació en cas de ser necessari.

7.2 Instruments d'avaluació

Incidents de Ciberseguretat																										
Unitats didàctiques		Act 1	Act 2	Act 3	Act 4	Act 5	Act 6	Act 7	Act 8	Act 9	Act 10	Act 11	Act 12	Act 13	Act 14	Act 15	Act 16	Act 17	Act 18	Act 19	Act 20	Act 21	Act 22	Act 23	Act 24	Act 25	Hores
1	Desenvolupament de plans de prevenció i conscienciació en ciberseguretat	x	x	x	x	x																					28
2	Auditoria d'incidents de ciberseguretat						x	x	x	x	x	x	x														28
3	Investigació dels incidents de ciberseguretat													x	x	x	x	x	x	x	x						30
4	Implementació de mesures de ciberseguretat																					x	x			x	18
5	Detecció i documentació d'incidents de ciberseguretat																							x	x	x	16
																											120

Continguts,criteris d'avaluació i instruments d'avaluació						
	Activitat	Hores	Contingut	CA	RA	Ins Av
Act 1	Gestió de contrasenyes Software i funcionament	2	C1.4	RA1-e	RA1	Practica 1
Act 2	Identificar Pishing	1	C1.4	RA1-e	RA1	Qüestionari
Act 3	Virus total	2	C1.4	RA1-e	RA1	Pràctica 2
Act 4	Pla de prevenció i concienciació. Preparació. Presentació	22	C1.1,C1.2, C1.3 i C1.5	RA1-a,b,c,d,e	RA1	Pràctica 3
Act 5	Test d'avaluació dels llocs de treball	1	C1.1,C1.2, C1.3, C1.4 i C1.5	RA1-e	RA1	Exercicis/Qüestionari 1
Act 6	Muntatge de escenari Wazuh Introducció a wazuh	4	C2.2	RA2-c,d,e	RA2	Practica 4
Act 7	Afegir agents de wazuh	3	C2.1	RA2-c,d,e	RA2	Pràctica 5
Act 8	Monitorització dels agents Configuració	6	C2.3, C2.4 i C2.5	RA2-c,d,e	RA2	Pràctica 6
Act 10	CLARA en su versión para el cumplimiento del EsquemaNacional de Seguridad ('ENS') para auditar un Sistema de Información.	4	C2.1	RA2-a	RA2	Pràctica 8
Act 11	Utilització de **Lynis** per a auditar un Sistema Linux.	4	C2.1, C2.2,C2.3,C2.4 i C2.5	RA2-a	RA2	Pràctica 9
Act 12	Prova escrita teòrica/pràctica sobre monitorització de sistemes	3	C2.1, C2.2,C2.3,C2.4 i C2.5	RA1-a,b,c,d,e RA2-a,b,c,d,e	RA1,RA2	Examen 1
Act 13	Identificar vulnerabilitats amb OpenVas Instal·lació Explicació Funcionament	6	C3.1,C3.2 i C3.3	RA3-a,b,c	RA3	Pràctica 10
Act 14	Anàlisis de correus electrònics Explicació Exemples	2	C3.5	RA3-c	RA3	Pràctica 11
Act 15	Investigar incident amb MITRE Utilització de MITRE	4	C3.4	RA3-d	RA3	Pràctica 12
Act 16	Investigar malware amb Virus Total	2	C3.4	RA3-d	RA3	Pràctica 13
Act 17	Investigar malware amb MITRE Comparacions i utilitzacions	4	C3.3 i C3.4	RA3-d	RA3	Pràctica 14

Act 18	Anàlisis exhaustiu d'un incident concret, contextualitzat en una empresa	4	C3.1,C3.2 i C3.3	RA3-a,e	RA3	Pràctica 15
Act 19	Analitzar diferents malware amb l'eina RENmux	4	C3.4	RA3-c	RA3	Pràctica 16
Act 20	Prova sobre la investigació d'incidents i de malware	4	C3.1,C3.2,C3.3, C3.4 i C3.5	RA3-a,b,c,d,e	RA3	Examen 2
Act 21	Implementació de mesures en materia de ciberseguretat amb AWS	4	C4.1,C4.2, C4.3, C4.4 i C4.5	RA4-a,b,c,d,e,f	RA4	Pràctica 17
Act 22	Implementació de mesures en materia de ciberseguretat amb SENTINEL	10	C4.1,C4.2, C4.3, C4.4 i C4.5	RA4-a,b,c,d,e,f	RA4	Pràctica 18
Act 23	Prova sobre la implemenatció de mesures de seguretat i detecció	2	C4.1,C4.2, C4.3, C4.4 i C4.5	RA4-a,b,c,d,e,f	RA4	Examen 3
Act 24	Detecció i documentació d'incidents de ciberseguretat amb LUCIA	6	C5.1,C5.2 i C5.3	RA5-a,b,c,d,e	RA5	Pràctica 19
Act 25	Detecció i documentació d'incidents de ciberseguretat amb SecutityOnion	10	C5.1,C5.2 i C5.3	RA5-a,b,c,d,e	RA5	Pràctica 20
Act 26	Prova de documentació d'incidents	2	C5.1, ,C5.2 i C5.3	RA5-a,b,c,d,e	RA4,RA5	Examen 4

7.3 Tipus d'avaluació.

La avaluacióseràcontinua i tindràen compte el progrés de l'alumne.

No obstant, encara que la avaluació es faça continua, hi ha tres moments en els que es materialitza durant el curs. Estos moments són:

- Avaluació inicial.
- Avaluació processal.
- Avaluació final.

> En el cicle presencial se requereix l'assistència, almenys, al 85% de classes i activitats programadas en el mòdul. Per tant, l'alumnat que supere el 15% de faltes d'assistència perdrà el dret a l'avaluació continua.

7.4 Criteris de qualificació.

Incidents de Ciberseguretat																												
	Avaluació 1													Avaluació 2														
	UD1					UD2							UD3									UD4			UD5			
RA	Act 1	Act 2	Act 3	Act 4	Act 5	Act 6	Act 7	Act 8	Act 9	Act 10	Act 11	Act 12	Act 13	Act 14	Act 15	Act 16	Act 17	Act 18	Act 19	Act 20	Act 21	Act 22	Act 23	Act 24	Act 25	Act 26	Perc per RA
RA1 (20 %)	10 %	10 %	10 %	60 %	10 %																						100,00 %
RA2 (20 %)						5 %	5 %	15 %	10 %	10 %	10 %	45 %															100,00 %
RA3 (20 %)													15 %	5 %	10 %	5 %	10 %	10 %	10 %	35 %							100,00 %
RA4 (20 %)																					20 %	30 %	50 %				100,00 %
RA5 (20 %)																								25 %	25 %	50 %	100,00 %

Figura 2: Avaluació

El mòdul estarà superat si s'han superat tots els Resultats d'Aprenentatge.

La nota final del mòdul s'obtindrà aplicant el pes corresponent a cadascun dels Resultats d'Aprenentatge.

Qm = 0,2*Qra1 + 0,2*Qra2 + 0,2*Qra3 + 0,2*Qra4 + 0,2*Qra5
Qm = Qualificació del mòdul QraN = Qualificació del Resultat d'Aprenentage N Totes les QRA han de ser >=5 per obtindre Qm.

Si s'utilitzen hores del mòdul en DUAL per a la formació en l'empresa, s'ajustarien els pesos dels RA's implicats i se sumaria la qualificació obtinguda en l'empresa segons el seu pes

Les qualificacions de les Unitats didàctiques s'obtenen de la qualificació dels resultats d'aprenentatge (RA), en funció dels instruments d'avaluació emprats. Tots els RA's s'hauran d'aprovar amb una qualificació superior o igual a 5 sobre 10 de forma independent. Com instruments d'avaluació Tenim:

- Exercicis i qüestionaris.
- Pràctiques.
- Examens o Proves escrites.
- Reptes.
- Projectes
- Casos d'estudi.

La superació de tots els resultats d'aprenentage implica la superació del mòdul en convocatòria ordinària. Si l'alumne no ha superat algun resultat d'aprenentatge o ha perdut el dret a l'avaluació continua, podrà presentar-se a la prova ordinària i/o extraordinària segons el calendari oficial del centre.

8 Espais i equipaments

D'acord amb el `RD 479/2020, de 7 d'abril`

La docència en un cicle d'especialització d'aquestes característiques requereix:

- Un espai formatiu amb una superfície mínima de 40 m2

- Un grau d'utilització no inferior al 50% del temps disponible per cada grup d'alumnes del cicle.

Amb els equipaments següents:

- Ordinador professor.
- Mitjans audiovisuals.Ordenador professor.
- Mitjans audiovisuals.
- Ordinadors alumnes.
- Sistemes de reprografia.
- Instal·lació de xarxa amb accés a Internet.
- Programari de control remot, Programari bàsic (sistemes operatius en xarxa),Programari d'aplicacions ofimàtiques, tractament d'imatges, entre altres, Programari específic per a virtualització, ferramentes de monitoratge basades en protocol snmp, ferramentes de monitoratge de servicis d'alta disponibilitat, entre altres
- Servidors de Fitxers, Web, Bases de dades i Aplicacions.
- Ferramentes de clonació d'equips.
- Tallafocs, detectors d'intrusos, aplicacions d'Internet, entre altres.
- Sistemes Gestors de Bases de dades. Servidors i clients.
- Entorns de desenrotllament, compiladors i intèrprets, analitzadors de codi font, empaquetadors, generadors d'ajudes, entre altres.
- Programari específic per a l'anàlisi, monitoratge i explotació de vulnerabilitats de xarxes i servicis, Programari específic de diagnòstic, seguretat, antivirus entre altres.Ordinadors alumnes.-

9 Mesures d'atenció a l'alumnat amb necessitats educatives especials.

En la Formació Professional qualsevol adaptació curricular ha de ser no significativa, per la qual cosa es realitzaran adaptacions sobre la metodologia i sobre el procés avaluador, podent-se modificar el format de pràctiques i exàmens, però mai suposarà cap modificació sobre els continguts mínims del mòdul.

Segons les circumstàncies i mantenint els mateixos objectius educatius és possible:

• Establir en cada unitat didàctica els diferents grups d'activitats.

• Plantejar metodologies i nivells d'ajuda diversos, segons el grau de coneixement previ detectat, el grau d'autonomia i responsabilitat i les dificultats detectades prèviament.

• Adaptar el material didàctic.

• Organitzar grups de treball flexibles, la qual cosa permetrà establir tasques de reforç, aprofundiment, etc, en funció de les diferents necessitats del grup.

10 Foment de la lectura i ús de les TIC

10.1 Foment de la lectura

El alumnes llegiran articles de revistes especialitzades online i webs de la matèria, articles d'opinió en blogs, tutorials de contingut relatiu als mòduls cursats etc, que els serviran tant per a completar la seua formació com per a adquirir hàbit de lectura.

Els canvis continuats en el món de les TIC fa que l'hàbit de cercar informació, llegir-se-la i entendre-la siga una de les competències bàsiques a desenvolupar. Per altra banda, aquest foment de la lectura s'ampliaria a l'ús i comprensió de la llengua anglesa.

10.2 Ús de les TIC

En quant a l'ús de les TIC es fomentarà:

• Realització de diagrames relacionats amb el contingut dels mòduls

• Elaboració de Documentació

• Participació en fòrums, blogs, wikis, etc.

• Accés a Internet

• Utilització de plataformes d'aprenentatge virtual (com 'AULES' de la Conselleria)

• Ús del correu electrònic

11 ACTIVITATS COMPLEMENTÀRIES.

Està previst, almenys, realitzar:

• Ponències, dutes a terme per professionals sobre temàtiques relacionades amb Ciberseguretat